SECURISER UN RESEAU WI-FI

Gilles Follic
Grégory Daniel

2 mars 2003

Table des matières

Chapitre 1

Introduction.

La sécurité est le principal point faible des réseaux Wi-Fi. Cela tient en premier lieu au caractère sans fil de Wi-Fi. Le support de transmission étant partagé, quiconque se trouvant dans la zone de couverture du réseau peut en intercepter le trafic ou même reconfigurer le réseau à sa guise.

Pour résoudre ce type de problème, le Wi-Fi implémente un certain nombre de mécanismes permettant d'empêcher toute écoute clandestine ainsi que toute tentative d'accès non autorisé.

Mais ces mécanismes présentent des vulnérabilités indéniables qu'il conviendra de corriger.

Aussi nous adopterons le plan suivant.

Dans un premier temps, nous positionnerons d'abord le réseau Wi-Fi parmi les réseaux sans fil et ferons une courte présentation de ce réseau.

Nous présenterons ensuite la problématique générale de la sécurité des réseaux sans fil et aborderont les attaques dont peut faire l'objet un réseau au sens large et un réseau Wi-Fi en particulier.

Nous présenterons enfin les solutions qui peuvent être apportées.

Une étude réalisée sur la vulnérabilité du réseau Wi-Fi est présentée en annexe ainsi qu'une présentation des différents algorithmes de cryptographie.

Chapitre 2

Positionnement du Wi-Fi par rapport aux réseaux sans fil.

En raison de leur facilité de déploiement et de leur coût relativement faible, les réseaux sans fil sont de plus en plus utilisés. Comme pour les réseaux filaires, il existe différents types de réseaux sans fil : les réseaux personnels " WPAN " (Wireless Personal Area Networks), les réseaux locaux " WLAN " (Wireless Local Area Networks), les réseaux métropolitains " WMAN " (Wireless Metropolitan Area Networks) et les reseaux nationaux " WWAN " (Wireless Wide Area Networks).

2.1 Les réseaux sans fil de type " WPAN ".

Les " WPAN " sont des réseaux sans fil de faible portée (quelques dizaines de mètres) qui, comme leur nom l'indique, sont des réseaux à usage personnel. Ils sont déjà présents sous différents noms :

- Bluetooth : Aussi connu sous la norme 802.15.1, Bluetooth est aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mb/s et une portée d'environ 30 mètres, Bluetooth offre de nombreuses possibilités grâce à la faible consommation de ses équipements. On trouve des composants Bluetooth dans beaucoup d'ordinateurs portables mais aussi dans de nombreux périphériques (appareils photos, téléphones portables, assistants personnels, ...). La norme 802.15.3 (Bluetooth2) qui devrait prochainement voir le jour est une version annoncée plus rapide et pouvant intégrer des mécanismes de sécurité, qui font actuellement défaut dans le protocole Bluetooth.
- ZigBee : Avec un débit plus faible que Bluetooth, la norme 802.15.4 (ZigBee) pourrait être très utilisée dans les années à venir. Les équipements

ZigBee moins consommateurs et moins onéreux que les équipements Bluetooth devraient trouver leur place dans les périphériques informatiques mais également en domotique (éclairage, système de sécurité, ...).

– Les liaisons infrarouges : Les liaisons infrarouges sont très utilisées pour des communications courte distance, cependant leur sensibilité aux perturbations empêche le développement de cette technologie dans les réseaux sans fil supérieurs à une distance d'une dizaine de mètres. Néanmoins, la portée d'interception peut-être très supérieure.

2.2 Les réseaux sans fil de type " WLAN " (norme 802.11)

La norme 802.11 dans les réseaux sans fil est la norme équivalente à la norme 802.3 (Ethernet) pour les réseaux filaires. Les prochaines sections de ce document seront principalement consacrées au " WLAN " et plus précisément à la norme 802.11b également appelée Wi-Fi (Wireless Fidelity).

La norme 802.11a, aussi appelée Wi-Fi5, a fait son apparition en France depuis le début de l'année. Elle dispose d'une largeur de bande de 300Mhz sur la bande de fréquence des 5 GHz ce qui autorise un débit de 54 Mbits/s.

Ces deux normes évolueront par la suite sous d'autres formes ayant pour noms 802.11.g, 802.11.f et 802.11.h ; si toutefois la norme de l'ETSI Hiperlan2 ne prend pas le dessus sur celles-ci.

2.3 Les réseaux sans fil de type " WMAN " (norme 802.16)

Encore à l'état de norme pour le moment, les réseaux sans fil de type " WMAN " ne sont pas des projets très avancés. Cependant la B.L.R. (Boucle Locale Radio) fait partie des réseaux sans fil de type " WMAN ". Sur la bande des 3,5 Ghz et des 26 Ghz, la BLR est une technologie sans fil capable de relier les opérateurs de téléphonie à leurs clients grâce aux ondes radio sur une distance de 4 à 10 kilomètres.

2.4 Les réseaux sans fil de type " WWAN ".

Bien que ces réseaux ne soient pas connus sous ce nom, ce sont aujourd'hui les réseaux sans fil les plus utilisés en France. Les technologies cellulaires tel que le GSM (Global System for Mobile Communication), le GPRS (General Packet Radio Service) et l'UMTS (Universal Mobile Telecommunication System) font ou feront partie de ce type de réseau.

Présentation du Wi-Fi (802.11b)

La norme 802.11b est plus connue sous le nom de " Wi-Fi " ou encore " Airport " chez Apple. La norme 802.11b, comme d'autres technologies propriétaires (HomeRF d'Intel, OpenAir) utilise la bande des 2,4 Ghz. La norme IEEE 802.11b a été adoptée en septembre 1999. Grâce à la technologie DSSS (Direct Sequence Spread Spectrum : envoi de l'information en simultanée sur plusieurs canaux en parallèle), elle peut atteindre des débits de 11Mb/s sur une portée de 300 mètres et plus.

2.5 Utilisation du Wi-Fi.

De nos jours les réseaux sans fil se développent très rapidement :

- pour des réseaux temporaires (salons, conférences, ...) ;
- pour des points d'accès haut débit dans les lieux publics (aéroports, gares, métros, ...) connus sous le nom de " hotspot " ou des lieux privés accueillant du public (hôtel, restaurant, ...) ;
- dans de nombreux organismes attirés par la souplesse des réseaux sans fil.

2.6 Caractéristiques techniques du Wi-Fi

La norme 802.11b utilise la bande des 2,4 Ghz, 14 canaux de transmission différents sont utilisables sur cette bande de fréquence (dont 4 canaux sont autorisés en France), ce qui permet à plusieurs réseaux de cohabiter au même endroit sans interférences.

Pour s'identifier auprès d'un réseau, les utilisateurs d'un réseau sans fil 802.11b utilisent un identifiant de réseau (SSID).

Le réseau local 802.11b est fondé sur une architecture cellulaire ou chaque cellule appelée BSS (Basic Service Set) est contrôlée par un " AP " (Access Point) également appelé pont, le tout formant un réseau appelé ESS (Extended Service Set). Ce mode de communication est appelé le mode " infrastructure ". Les ponts peuvent être reliés entre eux par des liaisons radios ou

filaires et un terminal peut alors passer d'un pont à un autre en restant sur le même réseau (concept du " roaming ").

Un pont sur un réseau sans fil équivaut à un concentrateur (hub) sur un réseau filaire. Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau. Si ce terminal scrute simultanément plusieurs canaux, il recevra alors le trafic de tous les réseaux qui l'entourent.
Le mode de communication " ad-hoc " est également disponible dans la norme 802.11b : il s'agit d'un mode point à point entre des équipements sans fil qui utilise des protocoles de routage proactifs (échange périodique des tables de routage pour la détermination des routes) ou des protocoles de routage réactifs (les routes sont établies à la demande). Il est possible de reconstituer un réseau à partir de ce mode de communication.

L'accès au réseau sans fil se fait par un protocole CSMA (Carrier Sense Multiple Access), quand un équipement du réseau veut émettre, il écoute le support de transmission et si celui-ci est libre, alors il émet.

Une fonction CRC32 (Cyclical Redundancy Check sur 32 bits) présente sur le protocole 802.11b permet de s'assurer de l'intégrité des données transmises via une liaison sans fil.
Cependant même si l'intégrité des données est préservée, l'authenticité n'est pas assurée par le CRC32.

Le 802.11b intègre en option un protocole de sécurité au niveau liaison appelé " WEP " (Wired Equivalent Privacy). Le WEP utilise l'algorithme de chiffrement RC4. La clef résultante de l'algorithme RC4 est d'une longueur de 64 bits ou 128 bits, cette suite d'octets est composée d'un vecteur d'initialisation (IV) sur 24 bits et d'une clef sur 40 ou 104 bits dépendante de ce vecteur d'initialisation et de la clef WEP initiale. Cette clef permet de générer un " pseudo aléa " d'une longueur égale à la taille maximale d'une trame. Le chiffrement est effectué par un OU EXCLUSIF (XOR) entre ce " pseudo aléa " et le message transmis décomposé en blocs de longueur identique.

2.7 Les avantages du Wi-Fi (802.11b)

Comme les autres réseaux sans fil, le “ Wi-Fi ” possède plusieurs avantages :

- la facilité de déploiement ;
- le faible coût d'acquisition ;
- la mobilité.

De plus, le Wi-Fi est interopérable avec les réseaux filaires existants et garantit une grande souplesse sur la topologie du réseau.

Attention, il est toutefois nécessaire de relativiser les trois avantages cités ci-dessus en fonction du niveau de sécurité que l'on compte appliquer sur son réseau (Cf section Sécurité du Wi-Fi).

Chapitre 3

Définition de l'objectif de sécurisation et exposé de la problématique générale de la sécurité réseau.

Le besoin de sécurisation d'une transaction entre un émetteur et un récepteur nécessite que les messages qui circulent possèdent les caractéristiques suivantes :

- le message doit être intègre, c'est-à-dire que le contenu du message à la réception doit être identique à celui du message à l'émission.
- le message doit être authentifié c'est-à-dire qu'on doit s'assurer que l'émetteur du message est bien celui annoncé à la réception,
- le message doit pouvoir être chiffré pour éviter qu'une personne intruse ne puisse lire le message.

Comme tout autre réseau, Wi-Fi peut être soumis à différents types d'attaques, soit pour en perturber le fonctionnement, soit pour intercepter les informations transmises. Le seul désavantage de Wi-Fi vient du support qu'il utilise, l'air ambiant qui le rend particulièrement vulnérable.

Pour éviter toute divulgation d'information, le trafic du réseau doit être codé de telle manière que quiconque le récupère ne puisse pas le déchiffrer.

Outre les écoutes clandestines, les principales attaques auxquelles peuvent être soumis un réseau sont celles qui visent à l'empêcher de fonctionner, jusqu'à le voir s'effondrer, ou y accéder et le reconfigurer à sa guise.

Les seules parades à ces types d'attaque sont la cryptographie, qui empêche les intrus d'accéder aux données échangées dans le réseau, et l'authentification qui permet l'identification et l'autorisation de toute personne voulant émettre des données.

Chapitre 4

Les attaques dont peut faire l'objet un réseau au sens large et le réseau Wi-Fi en particulier.

4.1 Typologie des nuisances.

4.1.1 Les messages ne sont pas intègres.

Les causes de la non intégrité des messages sont dûes essentiellement au manque de fiabilité des protocoles utilisés.

Les messages n'arrivent pas du tout,

Les messages n'arrivent pas dans leur intégralité,

Les messages arrivent déformés.

Ces causes peuvent être aussi au fait d'une malveillance lorsqu'un intrus s'infiltre dans le réseau.

4.1.2 Les messages ne sont pas transmis par le bon émetteur.

Dans ce cas, la plupart du temps c'est une personne A qui prend la place de la personne B déclarée émetteur ou se fait passer pour cette personne B.

Cela signifie que la personne A s'identifie comme étant la personne B.

4.1.3 Les messages sont lus par une personne non autorisée.

Dans ce cas, une personne, non destinataire du message prend connaissance du message.

Cette personne par exemple s'infiltre dans le réseau et pratique l'écoute par un matériel adapté.

S'il est difficile voir impossible d'éviter cette pratique, le seul remède résidera dans le fait que la personne intruse ne puisse comprendre le message, ce qui nous enverra vers la recherche de solution de cryptages tels qu'un décryptage soit impossible soit prend trop de temps ou de moyens pour pouvoir décourager l'intrus.

4.2 Les attaques.

Les attaques sur les réseaux ont en général des effets combinés qui comprennent un mélange des nuisances causées.

Les attaques peuvent être passives, comme dans le cas d'écoute d'un réseau visant à récupérer des informations en " craquant " les différents mots de passe et clés de chiffrement.

Dans d'autres cas, les attaques sont actives, l'attaquant tentant de prendre le contrôle des machines ou d'en détériorer certains équipements.

Les pratiques les plus connues sont les suivantes :

- **Attaques par déni de service (DOS).** Parmi les plus redoutées, cette attaque consiste à inonder le réseau de messages afin que le réseau ne puisse plus les traiter, voir jusqu'à ce qu'il s'effondre.
- **Attaque DOS dans le réseau sans fil**. Le but de cette attaque est d'empêcher le bon fonctionnement des réseaux sans fil. Dans un environnement radio, une attaque DOS peut consister en l'utilisation d'un équipement interférant avec le point d'accès ou les stations du réseau afin qu'elles ne puissent plus communiquer.
- **Attaque par force brute**. Consiste à tester toutes les combinaisons possibles afin de récupérer un mot de passe ou une clé de chiffrement utilisé dans le réseau.
- **Attaque par dictionnaire**. Est utilisé pour récupérer un mot de passe ou une clé en recourrant à une base de données contenant un grand nombre de noms.
- **Attaque par spoofing**. S'appuie sur l'usurpation d'une identité afin d'accéder au réseau et est généralement associé aux attaques par force brute ou par dictionnaire, qui permettent d'accéder à certaines infor-

mations.

- **Attaque sur l'exploitation des trous de sécurité**. De nombreux protocoles et système d'exploitation sont vulnérables du fait de leur conception. Ces failles peuvent être utilisées soit pour permettre à l'attaquant de s'introduire dans la machine ou dans le réseau, soit pour prendre le contrôle de la machine ou récupérer des données. Dans certains protocoles comme le WEP, de telles failles peuvent être utilisées pour accéder au réseau comme s'il n'était pas sécurisé.
- **Attaque par virus, vers et cheval de Troie.** Très connues, ces attaques permettent de détériorer des fichiers voir des composants de la machine, soit de prendre le contrôle d'une machine, (virus et vers), et d'en exploiter les ressources (cheval de troie).

Chapitre 5

Les solutions qui peuvent être apportées.

En raison de ces failles de sécurité, certaines entreprises ont interdit WI-Fi en leur sein. Force est pourtant de reconnaître que Wi-Fi est beaucoup plus sûr qu'un réseau Ethernet.

La meilleure manière de sécuriser aujourd'hui un réseau Wi-Fi est d'utiliser les mêmes mécanismes que les réseaux filaires, à savoir les serveurs d'authentification et les tunnels.

Dans la présentation des solutions, nous verrons d'abord les mécanismes de sécurité applicables aux réseaux Wi-Fi, ensuite nous verrons les failles de ces mécanismes, enfin nous proposeront les solutions pour contrer ces failles.

5.1 Les mécanismes de sécurité applicables aux réseaux Wi-Fi.

Pour permettre aux réseaux Wi-Fi d'avoir un trafic aussi sécurisé que les réseaux fixes, le standard 802.11 a mis en place un protocole appelé WEP (Wired Equivalent Privacy).

Ce protocole offre deux types de mécanisme : le chiffrement des données et l'authentification.

Tous deux repose sur l'utilisation d'une même clé secrète partagée. Le WEP est un système à clé symétrique, la même clé étant utilisé pour chiffrer et déchiffrer les données.

Chaque station et point d'accès possède une clé secrète partagée, qui peut être soit un mot de passe entré par l'utilisateur, soit une clé issue de ce mot de passe. La longueur de la clé peut-être de 40bits ou de 104 bits.

Le Wep est défini de manière optionnelle, et les stations et points d'accès ne sont pas obligés de l'utiliser. Les mécanismes définis dans le WEP sont eux aussi optionnels, une station pouvant utiliser le mécanisme d'authentification mais pas l'algorithme de chiffrement, et vice-versa.

Les principales caractéristiques du WEP sont les suivantes :

- **Confidentialité des données**. Utilisation du RC4 pour chiffrer les données et éviter l'ecoute clandestine.
- **Authentification.** Sécurisation du réseau en n'autorisant que les stations possèdent la bonne clé.

  Le WEP fournit en outre un contrôle de l'intégrité des données, qui permet de vérifier la validité des données lors des transmissions. Lorsque le WEP est utilisé, les performances s'en ressentent toutefois, et un réseau peut perdre jusqu'à 20% des ses capacités.

Remarque :

La baisse des performances du fait de l'utilisation de WEP dépend essentiellement du type de carte utilisée. Avec certaines cartes, la baisse n'est que de 5%, tandis qu'avec d'autres elle peut atteindre 20%, voir 59%.

5.1.1 L'accès au réseau.

L'identifiant du réseau, où SSID (Service Set ID), est le premier mécanisme de sécurité offert par le 802.11 pour le contrôle de l'accès au réseau. Le SSID est un nom que l'on donne à un réseau ou à un domaine. L'expression "nom de réseau " est surtout utilisée au moment de la configuration du réseau.

Toutes les stations et tous les points d'accès appartement à un même réseau doivent posséder ce SSI, que les stations soient en mode ad-Hoc ou en mode infrastructure.

Si une ou plusieurs stations veulent entrer dans un réseau sous le contrôle d'un point d'accès, elles doivent donner le SID au point d'accès. La ou les stations ne peuvent accéder au réseau que si ce SSID est correct. Le SSID est le seul mécanisme de sécurité obligatoire dans Wi-Fi.

ACL (Access Control List)

Pour restreindre encore plus l'accès au point d'accès, ce dernier contient une liste d'adresse MAC, appelée ACL (Access Control List).

L'adresse MAC est une adresse unique que possède toute carte Wi-Fi ou Ethernet. C'est par l'intermédiaire de cette adresse que la station peut-être reconnue dans le réseau. L'ACL permet de n'autoriser que les cartes dont les adresses MAC sont présentes dans la liste.

L'ACL est toutefois optionnelle et laissée à la charge de l'administrateur du point d'accès. Cette solution est rarement utilisée car, nous allons le voir par la suite, l'ACL est peu fiable.

5.1.2 Le chiffrement des données.

Le mécanisme de chiffrement du WEP s'appuie sur le RC4, développé par Ron Rivest en 1987 pour RSA Security. Le RC4 est divisé en deux parties :

- **Key Scheduling Algorithm**. Il s'agit d'une clé composée d'une clé secrète partagée concaténée avec un " Initialzation Vector ". Ce dernier est utilisé pour générer une table d'état comprenant un ensemble de permutations.
- **Séquence pseudo aléatoire**. La table d'état est placée dans un générateur de nombre aléatoire, ou PRNG (PseudoRandom Number Generator), fondé sur le RC4, qui créé une séquence pseudo aléatoire.

Le RC4 a pour principal avantage d'être très rapide par rapport aux autres algorithmes de chiffrement disponibles actuellement.

Le chiffrement.

Le mécanisme de chiffrement de données est divisé en deux parties : l'intégrité et le chiffrement proprement dit.

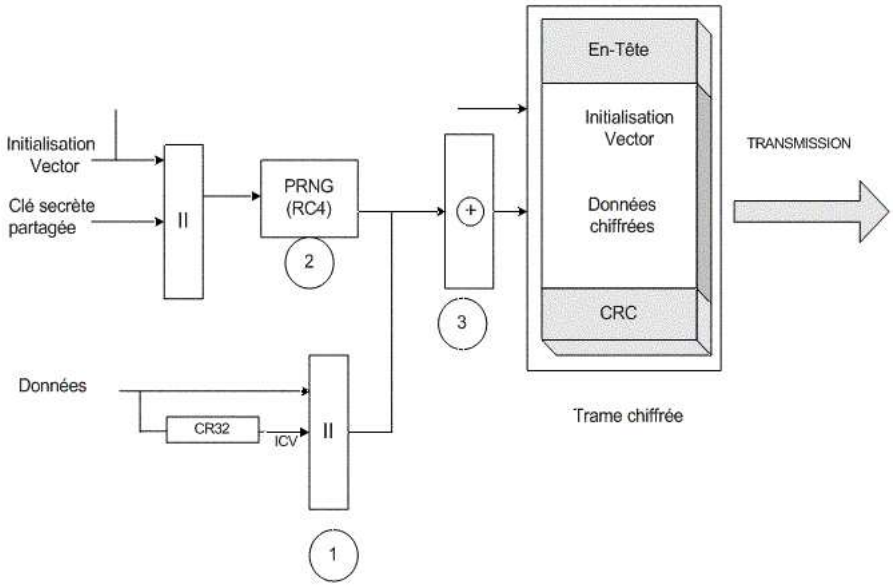
L'intégrité.

Avant de chiffrer les données, on effectue un calcul de l'intégrité des données, ou ICV (Integrity Check Value), grâce a un checksum non chiffré (CRC de 32 bits). La clé secrète n'est pas utilisée dans cette partie.

Les données sont ensuite concaténées avec l'ICV :

Données || ICV avec ICV = CRC (données)

Le processus de chiffrement.
Le processus de chiffrement est illustré ci-dessous.



1. La clé secrète partagée est concaténée avec un IV (Initialization Vector) de 24bits. Cet IV est variable mais doit etre réinitialisé après chaque utilisation.
2. La nouvelle clé de 64bits est placé dans le PRNG (PseudoRandom Number Generator). Le PRNG génère une séquence pseudo aléatoire permettant de chiffrer les données : RC4 (K || IV)
3. Une fois les deux premières parties terminées, les données sont chiffrées. Pour cela, on utilise un " ou exclusif " (XOR) :
   Données chiffrées = (données || ICV " ou exclusif " RC4 (k || IV).
4. Les données chiffrées sont transmises, et l'IV est ajouté à la trame.

Le chiffrement des données ne protège que les données de la trame MAC et non l'en tête ni le CRC. Cela permet aux autres stations d'écouter les trames, même chiffrés, afin d'en extraire des données utiles, telles que l'information de durée de vie pour le NAV.

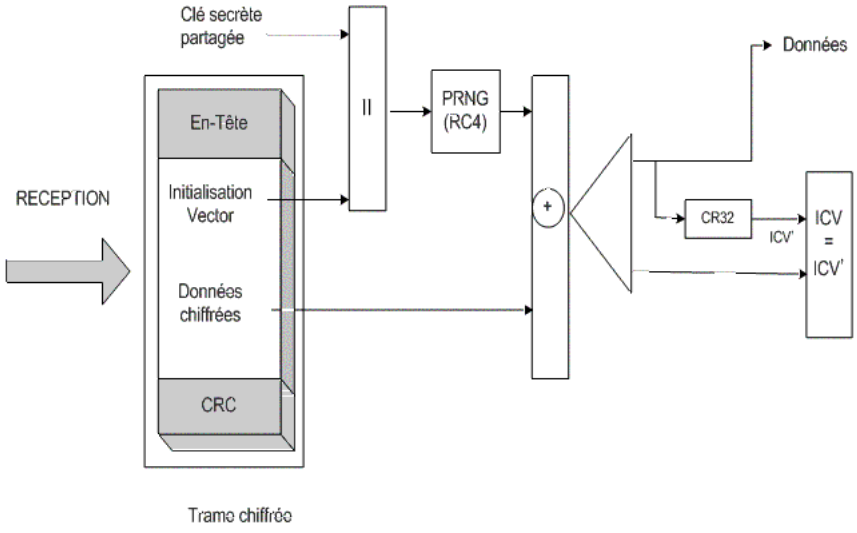
5.1.3 Le déchiffrement.

Comme pour le chiffrement, le mécanisme de déchiffrement est composé de deux parties : le déchiffrement proprement dit et le contrôle de l'intégrité des données.

Pour le déchiffrement, l'IV permet de retrouver la séquence de clés qui permet de déchiffrer les données. L'IV permet de retrouver la séquence de clés qui permet de déchiffrer les données. L'IV est concaténé avec la clé secrète, qui, une fois introduite dans le PRNG, donne la bonne séquence de déchiffrement des données. On obtient de la sorte les données déchiffrés ainsi que l'ICV.

Pour vérifier que l'opération de déchiffrement s'est déroulée correctement, un calcul d'intégrité est effectué sur les donnés déchiffrées. Cette nouvelle valeur, ICV', est comparée à l'ICV obtenu lors du déchiffrement. Si les valeurs d'ICV et d'ICV' sont différentes, c'est que les données sont erronées et doivent être retransmises.

Le schéma suivant illustre cette procédure :



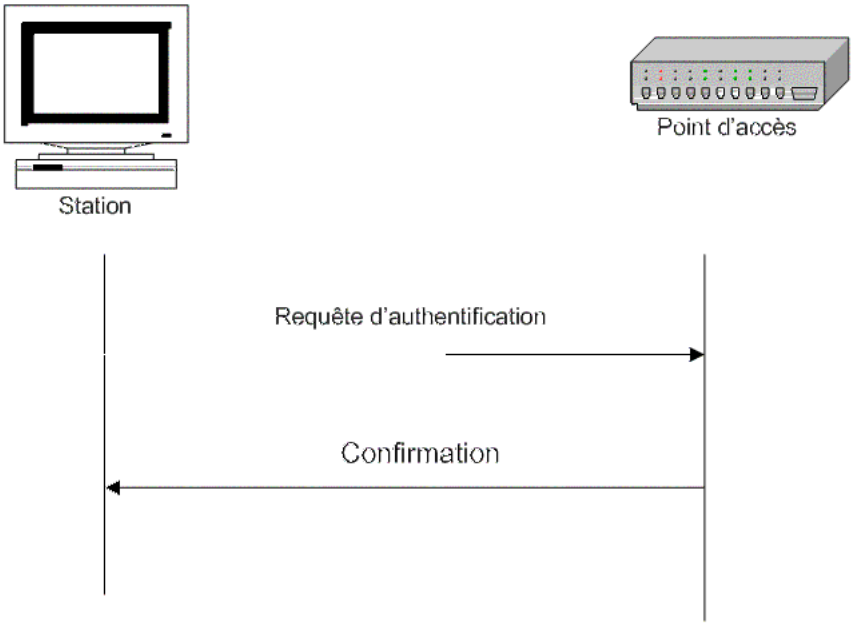
L'authentification.

Le mécanisme d'authentification utilise la clé partagée utilisée pour l'envoi des données chiffrées. IEEE 802.11 offre deux types de mécanisme d'authentification : Open system authentification et Shared Key authentification.

Open System Authentification.

Open System Authentification est le mécanisme d'authentification par défaut.

Ce mécanisme se déroule en deux étapes, comme illustré selon le schéma suivant :



1. Une station envoie une demande d'authentification.
2. La station reçoit une réponse négative ou positive.

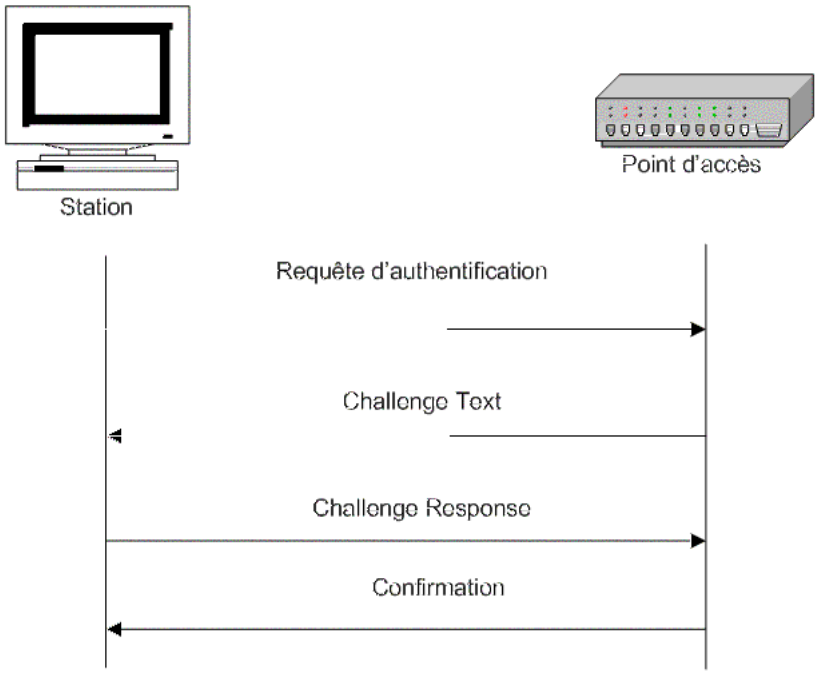
L'open System Authentification n'est pas un véritable système d'authentification, car n'importe quelle station peut s'authentifier auprès d'un point d'accès, aucune n'étant rejetée.

Shared Key authentification.

Ce mécanisme fournit un meilleur système d'authentification en utilisant un mécanisme de clé secrète partagée.

La clé secrète n'est pas envoyée en clair sur le réseau mais utilise le WEP pour être chiffrée. Ce mécanisme ne fonctionne évidemment que si les stations utilisent le WEP.

Cette authentification suit quatre étapes, comme illustré à la figure ci-dessous.



1. Une station qui souhaite s'associer à un point d'accès, lui envoie une trame d'authentification.
2. Lorsque le point d'accès reçoit cette trame, il retourne à la station une trame contenant 128 bits d'un texte aléatoire généré par l'algorithme WEP.
3. Après avoir reçu la trame contenant le texte, la station la copie dans une trame d'authentification et la chiffre avec la clé secrète partagée puis envoie le tout au point d'accès.
4. Le point d'accès déchiffre le texte chiffré avec la même clé secrète partagée et le compare avec le précédent. Si c'est le même, le point d'accès confirme à la station son authentification. Dans le cas contraire, il envoie une trame d'authentification négative.

Une fois l'authentification réussie, la station doit s'associer avec le point d'accès pour se connecter au réseau.

5.2 Les vulnérabilités et les failles de sécurité du réseau Wi-Fi.

5.2.1 La vulnérabilité de la technologie Wi-Fi.

De par sa technologie le Wi-Fi est un protocole qui **diffuse les données vers toutes les stations qui sont aux alentours**. Un utilisateur mal intentionné peut se placer dans le périmètre des équipements du réseau afin de récupérer les informations qui lui permettront d'avoir accès au réseau. De plus, ce périmètre peut-être mal configuré par défaut, auquel cas le réseau sera visible de l'extérieur des bâtiments.

La sensibilité au brouillage est une autre vulnérabilité induite par la technologie des réseaux sans fil. Elle peut entraîner un déni de service des équipements du réseau, voire la destruction de ces équipements dans le cas de bruit généré artificiellement.

Le dernier risque est lié plus à l'essor de cette technologie qu'à la technologie en elle même, il concerne la méconnaissance des utilisateurs vis à vis de leur équipement. Par exemple : Windows XP intègre par défaut la gestion des cartes sans fil, si l'ordinateur portable d'un utilisateur possède un équipement sans fil alors cet **ordinateur sera par défaut prêt à communiquer sur le réseau**.

5.2.2 La vulnérabilité des protocoles.

De base (sans algorithme de chiffrement) l'identifiant de réseau (SSID) n'est pas chiffré lors de la transmission des trames. Un utilisateur mal intentionné qui écoute le réseau peut obtenir le SSID lui permettant ainsi un accès au réseau. De plus, l'interprétation du SSID sur le réseau est souvent facilité par le fait que le SSID porte le nom du service ou de l'organisme utilisateur du réseau.

Afin de supprimer la vulnérabilité exposée ci-dessus, le protocole de chiffrement " WEP " à été mis en place. Cependant le processus de génération des clefs décrit dans le protocole présente quelques faiblesses :

- La première vulnérabilité concerne la faible longueur des clefs, certains équipements ne proposant que clefs de 40 bits. Cette faible longueur de clef facilite une attaque par " force brute " et permet d'obtenir la clef " WEP " dans un délai raisonnable.
- La seconde faiblesse de ce protocole a été identifiée par Fluhrer, Mantin et Shamir. En raison de l'implémentation de l'algorithme de chiffrement RC4, ils ont mis en évidence de larges ensembles de clefs dites " faibles

". Plusieurs outils disponibles sur Internet permettent à un utilisateur mal intentionné, non averti, d'obtenir le pseudo aléa généré.
– Afin de contrer cette vulnérabilité, certains composants suppriment ces clefs dites " faibles ". Dans ce cas une simple analyse statistique suffit à découvrir le pseudo aléa généré.

Même si l'utilisation de mécanisme de sécurité est un grand pas en avant, Wi-Fi comporte des failles, qui laissent libre cours à tous types d'attaques. En fait, c'est l'ensemble des mécanismes de sécurité de 802.11 qui comporte des failles : SSID (Service Set ID), ACL (Access Control Lis) et WEP (Wired Equivalent Privacy).

SSID (Service Set ID)

L'accés au réseau se fait par l'intermédiaire du SSID. Ce dernier est transmis périodiquement en clair par le point d'accès dans les trames balises. Il est assez facile de le récupérer, que ce soit par l'intermédiaire d'un sniffeur, logiciel permettant de récupérer toutes les données circulant sur un réseau.

Remarque :

Pour accéder à tout réseau dit ouvert, il suffit de spécifier comme SSID " any ". La station recherche alors tous les réseaux ouverts pour récupérer leur SSID.

Une nouvelle fonctionnalité permet d'éviter que le SSID ne soit transmis en clair sur le réseau par le point d'accès. Ce mécanisme appelé Closed Network, ou réseau fermé, interdit la transmission du SSID par l'intermédiaire des trames balises.

Lorsqu'un réseau est fermé, l'utilisateur doit entrer à la main le nom du réseau (SSID), alors que, dans un réseau ouvert, c'est la station de l'utilisateur qui s'associe directement au point d'accès sans qu'il soit nécessaire de la configurer manuellement.

Remarque :

Lorsque les stations sont ad-hoc , le SSID est transmis en clair par toutes les stations. Dans un tel cas, le réseau ne peut être fermé.

Même si le réseau est fermé, le SSID peut-être récupéré par d'autres moyens. En effet, le SSID étant transmis en clair pendant la phase d'association d'une station avec le point d'accès suffit de " sniffer " le réseau durant l'association pour le récupérer.

Un autre inconvénient du SSID vient du nom que lui donnent les constructeurs de matériels. Le SSID est généralement configuré au niveau des points d'accès. Chaque fabricant utilise et nomme un SSID par défaut, par exemple WaveLan Network chez Lucent et Tsunami chez Cisco.

Si le SSID n'est pas modifié chez l'utilisateur, n'importe quelle personne connaissant la marque du point d'accès peut tenter d'utiliser le SSID par défaut pour accéder au réseau. De plus si le SSID n'est pas modifié, il y a de fortes chances que le mot de passe utilisé ne le soit pas non plus.

ACL (Access Control List)

Le premier inconvénient de l'ACL est qu'il s'agit d'un mécanisme optionnel très rarement utilisé. De plus si une personne possède une adresse MAC qui ne se trouve pas dans la liste ACL, elle peut écouter le réseau et identifier les adresses MAC autorisées qui sont transmises en clair.

Une fois les adresses MAC autorisées connues, il est possible de substituer à sa propre adresse MAC une adresse autorisée. La plupart des drivers de carte WI-Fi le permettent.

WEP (Wired equivalent privacy)

Pour qu'un algorithme de chiffrement soit robuste, il faut que la clé utilisée pour chaque paquet envoyé soit différente. La faiblesse du WEP vient de la manière dont la clé de chiffrement est créée. Comme expliqué précédemment, cette clé est générée par la concaténation d'un vecteur d'initialisation et d'une clé secrète partagée. Or tout le problème vient de ce vecteur d'initialisation, qui est généralement initialisée à zéro à chaque nouvelle transmission. Ainsi une même clé peut être utilisée pour chiffrer les données.

C'est la faille du WEP, étant entendu qu'il est beaucoup plus facile de casser un algorithme de chiffrement lorsqu'une même clé est utilisée pour le chiffrement de données que dans le cas où une clé différente est utilisée pour chaque donnée transmise.

Différents logiciels utilisent cette faille pour permettre de récupérer la clé de WEP notamment les suivants :

- Airsnort (http ://airsnort.shmoo.com)
  Cet utilitaire libre fonctionnant uniquement sous Linux permet de récupérer la clé secrète partagée d'un réseau Wi-Fi sécurisé. Ce logiciel écoute le réseau afin de récupérer entre 100Mo et 1Go de données pour en déduire la clé.
  Comme Airsnort capture toutes les données qui circulent sur le réseau, le déchiffrement peut prendre quelques jours, voir quelques semaines selon la charge du réseau, jusque la quantité de données soit suffisante.
- Wepcrack(http ://sourceforge.net/projects/wepcrack).
  Comme airsnort, ce logiciel permet de déchiffrer le WEP. Il est toutefois moins complet qu'airsnort.

– Airopick(http ://www.wildpackets.com/products/airopick)
  Ce logiciel payant (2500$) permet de vérifier la sécurité d'un réseau et par voie de conséquence de déchiffrer le WEP ;
– Sniffer Wireless (http ://www.sniffer.com).
  Ce logiciel payant (9000$) permet de vérifier la sécurité d'un réseau Wi-Fi.

Actuellement de nombreuses solutions existent pour sécuriser un réseau Wi-Fi. Chaque fabricant propose pour ses cartes des versions améliorées du WEP. Dans la plupart des cas, il suffit de télécharger un patch et de l'appliquer à la carte, économisant ainsi l'achat de nouvelles cartes.

Conclusion sur la vulnérabilité du protocole WEP.

En conclusion
- La couche liaison de 802.11 n'offre aucune sécurité.
- Il faut utiliser des protocoles de sécurité supplémentaires tel que IPSec, SSL ou SSH et en aucun cas s'appuyer sur WEP pour assurer la sécurité.
- Toutes les entités utilisant 802.11 doivent être considérées comme externes et donc placées à l'extérieur du firewall.
- Il faut toujours avoir à l'esprit que toute personne se trouvant dans le rayon d'émission (et même au-delà grâce à des dispositifs amplifiants) peut être susceptible de communiquer sur le réseau en tant qu'utilisateur valide.

Les améliorations prévues.

RC4 Fast Packet Keying.

RSA Security, la société à l'origine du WEP, a amélioré son algorithme sous le nom de RC4 Fast Packet Keying. Ce nouveau WEP permet de créer une clé de chiffrement unique pour chaque trame envoyée, palliant ainsi l'inconvénient de la réinitialisation du vecteur d'initialisation.

Ce WEP+ devrait arriver sous la forme d'un patch pour les cartes Wi-Fi vers la fin de l'année 2002.

Le Fast Packet Keying fait appel à une table de hachage pour créer une clé unique permettant de coder chaque packet. Station et Points d'accès se partage cette clé de chiffrement d'une longueur de 128 bits, appelée TK (temporal Key). Le vecteur d'initialisation est toujours présent mais sa valeur est différente pour chaque TK.

La clé TK et l'adresse de l'émetteur, ou TA (Transmitter adress), sont mélangées pour former le TTAK (Temporal Transmitter Adress Key). De sorte chaque station utilise une clé différente pour le chiffrement des données. Le TTAK n'a pas à être calculé pour chaque transmission de données mais est généralement bufférisée par la station.

Le TTAK est ensuite mélangé avec le vecteur d'initialisation afin de créer une clé de chiffrement unique, la valeur du vecteur d'initialisation étant différente pour chaque trame envoyée.

IEEE 802.11i

Nouveau venu dans la famille 802.11, IEE802.11i apporte le tout nouveau système de chiffrement AES (Advanced Encryption Standard), destiné à remplacer le RC4 et le DES pour tout ce qui concerne le chiffrement et le mécanisme d'authentification. Utilisé par toutes les administrations américaines, AES sera sans doute la référence en cryptographie durant les années à venir.

AES est un algorithme par bloc réputé rapide et surtout fiable. S'il est possible de percer le DES en une seconde, il faudrait plus de cent milliards d'années pour percer l'AES. Malheureusement, il demande une puissance de calcul que ne possèdent pas les cartes Wi-Fi actuelles.

Il faudra donc renouveler cartes et points d'accès pour bénéficier de ce nouvel algorithme, ce qui risque de couter cher aux entreprises et particuliers déjà équipés.

L'implémentation d'AES dans les cartes Wi-Fi ou Wi-Fi 5 n'est pas pour tout de suite et il faudra attendre fin 2003 pour pouvoir réellement l'utiliser.

5.2.3 Vulnérabilités lors de l'implémentation.

La norme 802.11b n'offre pas de mécanisme de distribution de clefs, dans la plupart des cas il existe une seule clef pour tout le réseau, placée sur chaque équipement du réseau (dans des fichiers ou encore sur les composants du réseau sans fil, comme par exemple, une carte pcmcia, une carte réseau sans fil, ...). C'est cette clef qui permet de s'authentifier sur le réseau. Un utilisateur mal intentionné qui récupère cette clef (vol physique d'un appareil ou déchiffrement) gagne ainsi l'accès au réseau sans fil.

Plusieurs vulnérabilités découlent de l'apparente facilité de déploiement des réseaux sans fil :

- La mise en place d'un réseau sans fil est réalisée par une personne extérieure à l'équipe réseau et à l'équipe sécurité des systèmes d'information. Toutes les règles de bases pour se protéger des vulnérabilités décrites ci-dessus peuvent ne pas être appliquées.
- La configuration par défaut n'est pas modifiée lors de l'installation ce qui permet par exemple : l'administration des bornes via une interface web, l'entrée sur le réseau en utilisant le SSID par défaut, ...

5.3 Les solutions préconisées.

Pour faire face aux vulnérabilités de l'ensemble du mécanisme de sécurité de 802.11, il convient d'utiliser les mêmes mécanismes que le réseau filaire à savoir les serveurs d'authentification et les tunnels.

Nous terminerons par une série de conseils pratiques.

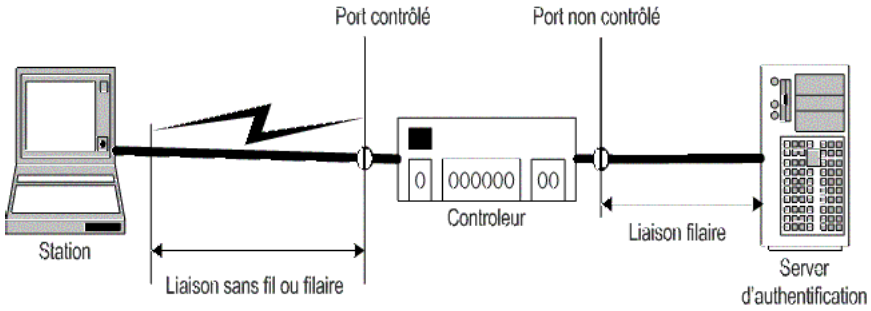
5.3.1 Le protocole IEEE 802.1X et EAP.

IEEE 802.1x, aussi appelé Port-Based Network Access Control, a été ratifié en 2001 pour l'authentification et la gestion des clés et est pleinement supporté par Windows XP.

La notion de port 802.1x définit tout type d'attachement à une infrastructure d'un réseau local. Dans le cas de Wi-Fi, l'association entre une station et un point d'accès est définie comme un port par 802.1x. Dans le cas d'Ethernet, la connexion de deux machines est considérée comme un port par 802.1x.

802.1x est un protocole d'authentification qui fonctionnent aussi bien dans les réseaux filaires tel qu'Ethernet que dans les réseaux sans fil comme Wi-Fi. L'architecture de 802.1x est constituée des trois éléments suivants illustrés ci-dessous :

- Un client, qui correspond à l'utilisateur qui voudrait se connecter au réseau via sa station.
- Un contrôleur, généralement un point d'accès dans le cas Wi-Fi, qui relaie et contrôle les informations entre tout demandeur et le serveur d'authentification.
- Un serveur d'authentification, qui authentifie l'utilisateur.

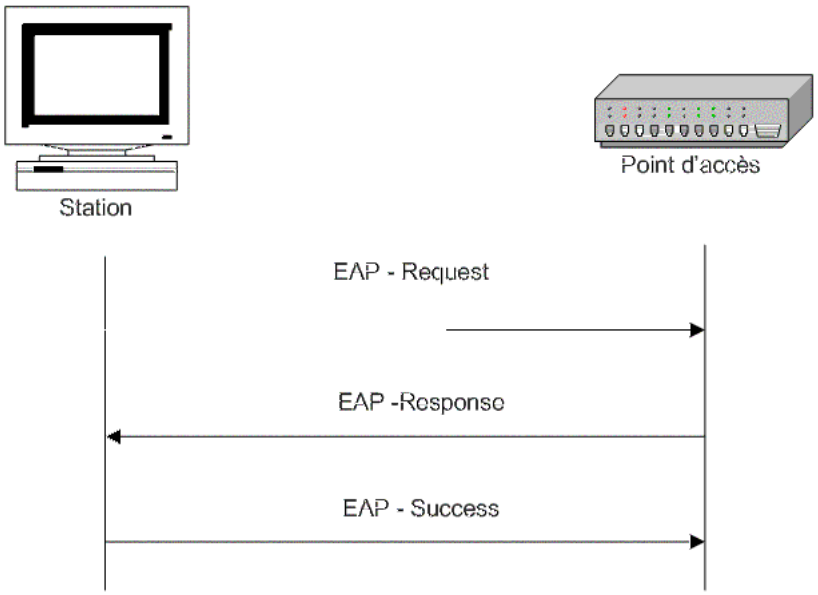


Pour chaque port, le trafic du réseau peut être ou non contrôlé. Entre le client et le contrôleur, le port est contrôlé de telle sorte que seule des messages d'authentification de type requête réponse sont transmis, tout autre type de trafic étant rejeté. Entre le contrôleur et le serveur d'authentification, en revanche, tout type de trafic est accepté.

L'authentification s'appuie sur le protocole EAP (Extensible Authentification Protocol). Developpé à l'origine en tant qu'extension de PPP (Point-to-Point Protocol), EAP est actuellement utilisé par de nombreux constructeurs, qui l'incorporent dans leurs produits Wi-Fi.

EAP supporte différents types de schémas d'authentification, comme le EAP-MD5, qui utilise un challenge MD5, ou EAP-TLS (Extensible Authentification Protocol-Transport Layer Security), TLS étant une extension de SSL.

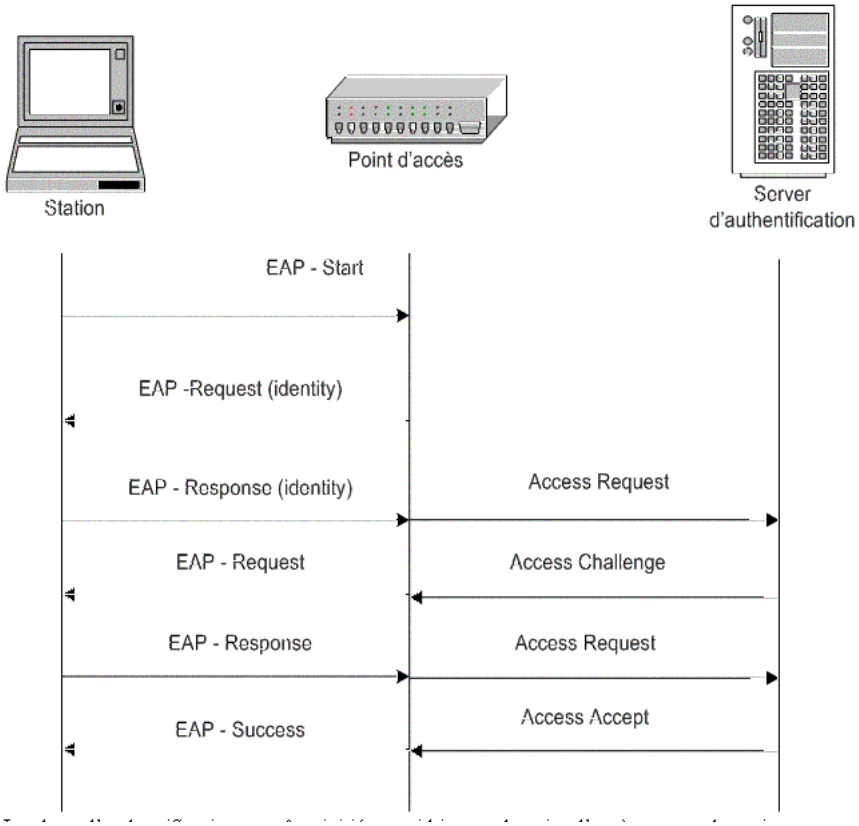
EAP peut être utilisé hors du cadre de 802.1x. Dans Wi-Fi, par exemple, un point d'accès peut utiliser le protocole EAP seul afin d'authentifier toute station voulant s'y associer. L'échange de messages EAP pour l'authentification d'une station auprès d'un point d'accès se schématise de la façon suivante :



Dans le cas où seul EAP est utilisé comme protocole d'authentification, le point d'accès est à l'initiative de la phase de négociation. Pour cela, le point d'accès envoie une ou plusieurs requêtes auxquelles doit répondre la station. La phase d'authentification se termine soit par un message EAP-Success, qui

garantit que la station est authentifiée, soit par un message EAP-Failure, et dans ce cas la station n'est pas authentifiée.

802.1x utilise un serveur d'authentification vers lequel le point d'accès relaye les informations illustrées de la façon suivante :



La phase d'authentification peut être initiée aussi bien par le point d'accès que par la station. Dans notre cas, c'est la station qui est l'initiative. Après avoir reçu la demande d'authentification, le point d'accès demande à la station de s'identifier par une EAP-Request (identity). Dès que la station s'identifie auprès du point d'accès par une EAP-response(Identity), cette requête est transmise au serveur d'authentification (Access Request). Dès lors, le point d'accès ne fait que relayer les messages sous forme de requêtes EAP entre le serveur d'authentification et la station.

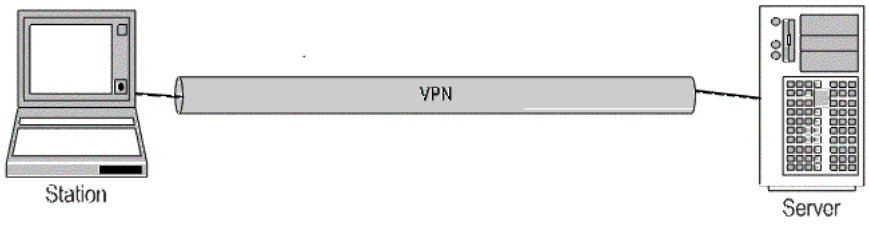
Généralement, la station et le serveur d'authentification se partagent un secret (clé, certificat). Dès que le serveur d'authentification reçoit une requête du point d'accès, pour une station donnée, il envoie un message Access Challenge contenant un challenge à la station. Ce challenge ne peut être résolu que par le secret partagé entre la station et le serveur d'authentification. Si le challenge n'est pas résolu, la station ne peut pas s'authentifier ;

s'il l'est, le serveur d'authentification authentifie la station, qui peut dès lors se connecter au réseau par l'intermédiaire du port contrôlé situé entre elle et le point d'accès.

Tout type de serveur supportant EAP peut être utilisé comme serveur d'authentification, mais le plus répandu reste RADIUS (Remote Authentification Dial-in-User Server).

Les réseaux privés virtuels

Le rôle des réseaux privés virtuels, ou VPN (Virtual Private Network) est de fournir un tunnel sécurisé de bout en bout entre un client et un serveur schématisé de la façon suivante :



Les VPN permettent, entre chose, d'identifier et d'autoriser l'accès ainsi que de chiffrer tout trafic circulant dans le réseau.

A ce jour, IPsec est le protocole le plus utilisé dans les VPN, Standard de référence, IPsec s'appuie sur différents protocoles et algorithmes en fonction du niveau sécurité souhaité :

- authentification par signature électronique à la clé publique (RSA) ;
- contrôle de l'intégrité par fonction de hachage (MD5) ;
- confidentialité par l'intermédiaire d'algorithmes symétriques, tels que DES, 3DES, RC5, IDEA ou Blowfish.

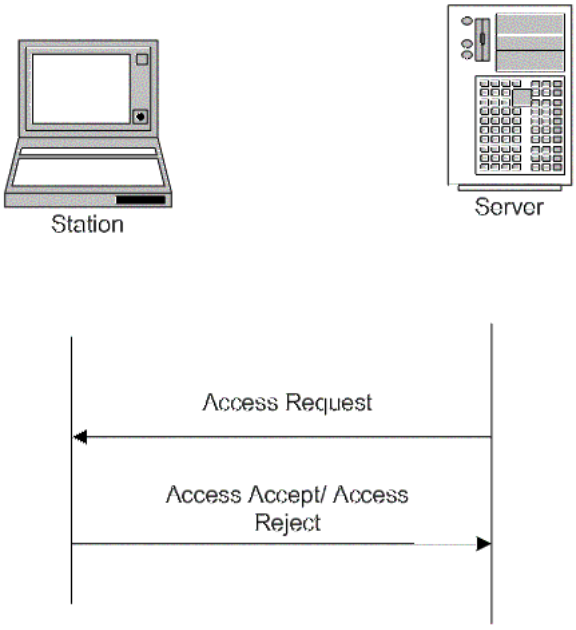
A ce jour, l'utilisation d'un VPN est la manière la plus fiable de sécuriser un réseau sans fil. C'est aussi la méthode la plus utilisée.

RADIUS (Remote Authentification Dial-in User Service)

RADIUS est un protocole centralisé, permettant l'autorisation et l'authentification de l'utilisateur. Conçu à l'origine pour l'accès à distance, il est aujourd'hui utilisé dans nombre d'environnements, tels que les VPN et les points d'accès Wi-Fi, et est devenu un standard IETF(RFC 2865).

RADIUS est situé au dessus du niveau 4 de l'architecture OSI. Il utilise un protocole de transport UDP pour des raisons évidentes de rapidité et repose sur une architecture client serveur.

Comme le montre le schéma qui suit :



Le client envoie des attributs de connexion auprès du serveur. L'authentification entre le serveur et le client se fait par l'intermédiaire d'un secret partagé, qui est généralement formé d'une clé et des attributs du client. Pour s'authentifier, le serveur envoie un challenge au client, que seul le secret partagé peut résoudre. Il vérifie les attributs envoyés par le client et la réponse au challenge et, s'ils sont corrects, accepte le client.

Ce protocole est implémenté des la plupart des points d'accès en vente aujourd'hui et constitue l'une des pièces maîtresses du protocole IAPP de gestion des handovers et de la norme 802.1x.

Gestion dynamique des clés.

Comme expliqué précédemment, la faiblesse du WEP vient de sa gestion des clés de chiffrement.

Certains constructeurs proposent dans leurs produits Wi-Fi un mécanisme de gestion dynamique des clés de chiffrement, toujours fondé sur le WEP. Ce mécanisme permet à chaque période de temps, définie soit par le constructeur, soit par l'utilisateur, de changer de clé de chiffrement. Ce temps, qui se compte généralement en dizaines de minutes, ne permet pas à un hacker de récupérer assez d'informations pour casser la clé.

5.3.2 Conseils pratiques.

De façon générale.

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter et d'accéder à ce réseau. Ceci est à-peu-près équivalent à connecter son réseau filaire à l'Internet sans l'avoir sécurisé au préalable. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité d'un réseau sans fil peut être réalisée à différents niveaux.

La sécurité d'un réseau sans fil commence par sa gestion. Gérer un réseau sans fil nécessite de s'appuyer sur une équipe ayant une bonne connaissance des réseaux et de la sécurité des systèmes d'information.

Sécurité des bornes.

Supprimer la configuration par défaut des " AP " est une première étape dans la sécurisation de son réseau sans fil. Pour cela il est nécessaire de :

- modifier la clef WEP et l'identifiant réseau (SSID) installés par défaut ;
- désactiver les services d'administration disponibles sur l'interface sans fil ;
- régler la puissance d'émission du pont (AP) au minimum nécessaire (cette conditon n'empêche pas un utilisateur mal intentionné muni d'un matériel spécifique d'écouter le réseau à distance).

Pour augmenter la sécurité il est également possible sur certains équipements de filtrer les adresses MAC ayant le droit de communiquer avec le pont. Cette liste devra être reproduite sur chaque pont du réseau sans fil si l'on désire garder toute la mobilité du réseau. Malgré cela, il sera toujours possible à un utilisateur mal intentionné de récupérer le trafic échangé entre deux machines (même si le protocole WEP est actif), voire de simuler une adresse MAC interceptée, si celui-ci se trouve dans le périmètre du réseau.

Sécurité des équipements.

La norme 802.11i devrait temporairement permettre de remédier à quelques un des problèmes de sécurité que peuvent présenter les normes 802.11b et les autres normes 802.11. La norme 802.11i compatible avec la norme 802.11b comprend le protocole TKIP (Temporal Key Integrity Protocol). Les points forts de ce protocole sont :

- des clefs WEP dynamiques différentes à chaque session ;
- des vecteurs d'initialisation sur 48 bits générés avec des règles définies ;
- le contrôle d'intégrité sur les données et les en-têtes est effectué par l'algorithme MIC (Message Integrity Code).

Des équipements utilisant ce protocole sont déjà présents sur le marché (ponts et cartes).

Dans un futur proche, le protocole AES devrait remplacer le protocole RC4 pour le chiffrement des clefs WEP.

Sécurité sur le protocole

Même si le chiffrement au niveau liaison (le WEP) de la norme 802.11b présente des faiblesses structurelles, il est nécessaire de l'utiliser en l'associant à des moyens supplémentaires permettant d'authentifier l'utilisateur sur le réseau comme par exemple la mise en place d'un réseau privé virtuel.

La mise en place d'un réseau privé virtuel est pour le moment la solution qui est la plus sécurisée. Dans l'attente de la future norme 802.1x (voir section suivante) il est donc recommandé de mettre en place cette solution.

La future norme 802.1x

Cette norme plus générale que le norme 802.11i permet de résoudre les problèmes d'authentification et de chiffrement posés par les normes 802.11, 802.3 (Ethernet) et 802.5 (Token Ring). Cette norme incorpore des fonctionnalités qui ne sont pas présentes sur la norme 802.11 :

- Le chiffrement : avec des clef de 128 bits différentes pour chaque nouvelle session.
- L'authentification : le protocole 802.1x prévoit l'utilisation de protocole d'authentification comme EAP (Extensible Authentification Protocol), RADIUS (Remote Authentification Dial-In User Service) ou bien TLS (Transport Layer Security) pour l'authentification mutuelle.

Le protocole LEAP (Light Extensible Authentification Protocol), également présent dans la norme 802.1x, est un protocole d'authentification s'appuyant sur le protocole EAP. Ce protocole est déjà implanté dans des équipements

CISCO sans fil. Il permet l'authentification entre le client et l'“ AP ” sur les réseaux sans fil.

Sécurité après la mise en place du réseau sans fil

Afin de conserver une sécurité satisfaisante de son réseau sans fil, il est nécessaire d'appliquer les mêmes procédures que pour les réseaux filaires, à savoir :

- Informer les utilisateurs : la sécurité d'un réseau passe avant tout par la prévention, la sensibilisation et la formation des utilisateurs ;
- Auditer son réseau : l'audit d'un réseau sans fil s'effectue en deux parties. Un audit physique pour s'assurer que le réseau sans fil ne diffuse pas d'informations dans des zones non désirées et qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser. Un audit informatique, comme pour les autres réseaux, pour s'assurer que le degré de sécurité obtenu est bien égal à celui désiré.
- Surveiller son réseau : la surveillance d'un réseau sans fil peut, elle aussi, s'effectuer à deux niveaux. La surveillance au niveau IP avec un système de détection d'intrusions classique (prelude, snort, ...) et la surveillance au niveau physique (sans fil) avec des outils dédiés (PrismDump, AirTraf, AirIDS, ...).

Chapitre 6

Conclusion.

Malgré des problèmes de sécurité intrinsèques, les réseaux sans fil continueront probablement à se développer dans le futur. Il est donc important de connaître les problèmes inhérents à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes. Les réponses aux problèmes de sécurité devraient être améliorées dans les prochaines normes de l'IEEE.

Chapitre 7

ANNEXE 1 : La vulnérabilité du protocole WEP

Approche théorique

De façon très succincte, le chiffrement utilisé par WEP peut-être décrit comme suit : la clé partagée est notée K. Au moment de la transmission des données M, celles-ci sont d'abord concaténées avec leur checksum c(M). Parallèlement à cela le vecteur d'initialisation est concaténé à la clé K, et passé en entrée à la fonction de chiffrement RC4. Le résultat subit un XOR avec les données :

$$C = (M \,||\, c(M)) \text{ XOR } RC4\ (IV \,||\, K)$$

La structure du RC4 se compose de 2 parties distinctes ; la première, ou key scheduling algorithm, génère une table d'état S à partir des données secrètes, à savoir soit 64 bits (40 bits de clé secrète et 24 bits d'IV) ou 128 bits (104 bits de clé secrète et 24 bits d'IV). La deuxième partie de l'algorithme RC4 est le générateur de données en sortie, qui utilise la table S et 2 compteurs. Ces données en sortie forment une séquence pseudo-aléatoire.

Fluhrer, Mantin et Shamir présentent 2 faiblesses dans la spécification de l'algorithme RC4. La première repose sur le fait qu'il existe de larges ensembles de clés dites faibles, c'est-à-dire des clés dont quelques bits seulement suffisent à déterminer de nombreux bits dans la table d'état S (avec une forte probabilité), ce qui affecte directement les données produites en sortie ; c'est l'attaque nommée "invariance weakness".

La deuxième attaque de Fluhrer, Mantin et Shamir est la "known IV attack ". Elle nécessite la connaissance de l'IV ce qui est le cas puisqu'il circule

en clair sur le réseau, et la connaissance du premier octet de M (à deviner). Dans un certain nombre de cas (“ les cas résolus ”, suivant l'expression de Fluhrer, Mantin et Shamir) , la connaissance de ces 2 éléments permet de déduire des informations sur la clé K.

Selon les auteurs, ces 2 attaques sont applicables et peuvent permettre une récupération complète de la clé avec une efficacité bien supérieure à l'attaque par recherche exhaustive.

Mise en pratique

L'implémentation de cette deuxième attaque par Stubblefield, Ioannidis et Rubin [2] a pris une semaine, requis 2h de codage et 100$ d'investissement. Leur principale difficulté a été de deviner le premier octet des données brutes (le plaintext M) ; or malgré les différents types de protocoles utilisés (notamment de l'ARP et de l'IP), il s'est avéré que 802.11 rajoute une couche supplémentaire en encapsulant tous ses paquets (header SNAP de 802.2). Ainsi, tous les paquets capturés commençaient par le même octet 0xAA.

Selon les auteurs, 256 cas “résolus” suffisent pour retrouver l'intégralité de la clé de 128 bits ; ils ont également optimisé leur méthode d'attaque et ont estimé qu'un jour ou deux suffiraient à un attaquant inexpérimenté pour arriver au même résultat. Une des optimisations a consisté à tester directement des caractères simples, c'est-à-dire mémorisables par les utilisateurs. En effet, d'une part la passphrase était utilisée à l'état brut (sans hachage) dans le cas étudié, et d'autre part cette passphrase se devait d'être suffisamment simple pour être retenue par tous les utilisateurs.

Chapitre 8

ANNEXE 2 : La cryptographie.

Le fait de rendre un texte ou un message incompréhensible grâce à l'utilisation d'un algorithme n'est pas nouveau. Les égyptiens comme les romains utilisaient déjà des méthodes permettant de coder un texte ou un message. Ces techniques, relativement simples à l'origine ont évolué, et c'est depuis la seconde guerre mondiale que la cryptographie a conquis le statut de science.

8.1 Principe de base

Une clé de cryptage est utilisée pour coder un texte en clair. Le texte chiffré est alors envoyé au destinataire. Ce dernier utilise une clé de décryptage afin de reconstituer le texte en clair. A tout moment pendant la transmission un individu peut récupérer le texte chiffré, appelé cryptogramme et essayer de le déchiffrer par diverses méthodes.

Remarque :

La cryptographie ne s'attelle qu'à la conception et aux méthodes de cryptage. L'action de chercher et déchiffrer un texte chiffré s'appelle la cryptanalyse. La cryptologie désigne pour sa part l'étude de la cryptographie et de la cryptanalyse.

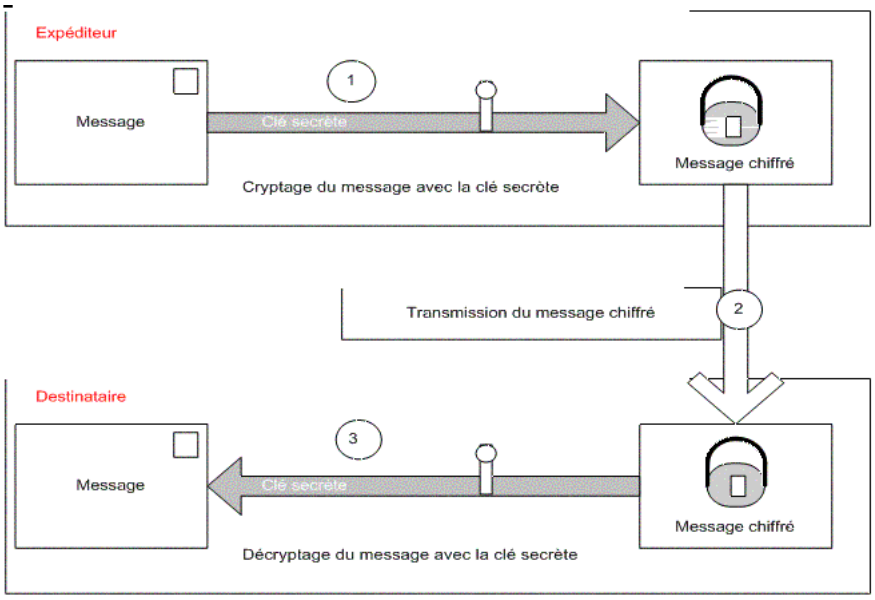
En France, il existe une réglementation stricte sur la longueur des clés utilisées pour le chiffrement.Une clé d'une longueur maximale de 40bits peut être utilisée pour tout usage public ou privé. Pour l'utilisation privée, la longueur de la clé ne peut excéder 128bits.

Il existe deux techniques de cryptographie, la cryptographie a clé symétrique et la cryptographie asymétrique, plu connu sous le nom de cryptographie à clé publique.

8.2 La cryptographie à clé symétrique

La cryptographie à clé symétrique est fondée sur l'utilisation d'une clé unique, qui permet à la fois de chiffrer et de déchiffrer les données. Toutes les personnes voulant se transmettre des données de manière sécurisée doivent donc partager un même secret : la clé.

Ce processus est schématisé de la façon suivante :



La faille de ce système réside évidemment dans la transmission de cette clé secrète partagée, tout le problème venant de la manière dont est transmise la clé entre l'émetteur et le récepteur.

Différents algorithmes de cryptographie à clé symétrique ont été développés, notamment DES (Data encryption Standard), IDEA (International Data encryption Algorithm) et la serie RC2 à RC6.

8.3 Algorithmes de cryptographie à clé symétrique

DES

L'algorithme DES a été développé dans les années 70 conjointement par IBM et la NSA (National security Agency). Le DES est algorithme de chiffrement dit par bloc, la longueur de la clé utilisé est fixe, 40 ou 56bits. Le rôle du DES est d'effectuer un ensemble de permutations et de substitutions entre la clé et le texte à chiffrer de façon coder l'information.

Le mécanisme de chiffrement suit plusieurs étapes :

le texte à chiffrer est fractionné en blocs de 64bits (8bits sont utilisé pour le contrôle de parité).

Les différents blocs sont soumis à une permutation dite initiale.

Chaque bloc est divisé en deux parties de 32 bits : une partie droite et une partie gauche.

Seize rondes sont effectuées sur les demi blocs.Une ronde correspondant à un ensemble de permutations et de substitutions. A chaque ronde, les données et la clé sont combinées.

A la fin des seize rondes, les deux demi blocs droit et gauches sont fusionnés, et une permutation initiale inverse est effectuée sur les blocs.

Le déchiffrement s'opère dans l'ordre inverse du chiffrement, mais en utilisant toujours la même clé.

Le DES était jusqu'à maintenant la référence en matière cryptographique à clé symétrique. De nombreux systèmes l'utilisaient et l'utilisent encore actuellement. Le protocole d'échange d'information sécurisé par Internet SSL (Secure Sockets Layer) v1.0 l'utilise, par exemple, avec une clé 40bits.

Considéré comme peu fiable, le DES n'est plus utilisé depuis 1998. Son algorithme de chiffrement a été repris et amélioré.

3-DES

3-DES ou triple-DES utilise 3 DES à la suite. Les données sont donc chiffrés puis déchiffrés puis chiffrés avec deux ou trois clés différentes. La clé 3-DES peut avoir une tailles de 168bits, ce qui ne lui permet pas d'être utilisée en France. Le 3-DES est considéré comme raisonnablement fiable.

IDEA (International Date Encryption Algorithm).

IDEA (International Date Encryption Algorithm) est un algorithme d'une longueur de clé de 128bits. Le texte à crypter est découpé en quatre blocs. Sur chaque sous bloc, huit rondes sont effectuées. Chaque ronde est une combinaison de " ou " exclusif, d'addition modulo 2 puissance 16 et de multiplication 2 puissance 16. A chaque ronde, les données et la cl& sont combinés. Cette technique rend l'IDEA particulièrement sécurisé.

L'algorithme IDEA est implémenté dans PGP (Pretty Good Privacy), le logiciel de cryptage le plus utilisé au monde.

RC2

L'algorithme RC2 a été développé par Ron Rivest, d'où son nom de Ron's Code 2. Il s'appuie sur un algorithme par bloc de 64bits et est deux voir trois fois plus rapide que le DES, avec une longueur de clé maximale de 2048bits.

RC4

Le RC4 (Ron's Code 4) n'utilise plus de bloc mais chiffre par flot. Sa spécificité réside dans l'utilisation de permutations pseudo aléatoires pour chiffrer et déchiffrer les données. Il est encore plus rapide que RC2. Comme le RC2, l'algorithme du RC4 est la propriété de RSA security.

Le RC4 est utilisé dans SSL v2.0 et SSL 3.0 pour sécuriser les connexions ainsi que dans le protocole WEP d'IEEE 802.11.

RC5 et RC6

Autre algorithme propriétaire de RSA security, le RC5 est un algorithme de chiffrement par bloc, avec une taille de bloc variable, comprise entre 32 et 128bits, un nombre de ronde variable, compris entre 0 et 255, et une longueur de clé dynamique, comprise entre 0 et 2040bits.

Le RC6 est une amélioration du RC5, dont il utilise les caractéristiques. La seule différence porte sur l'ajout de nouvelles opérations mathématiques au niveau des rondes.

Blowfish

Commes DES, Blowfish est un algorithme de chiffrement par bloc 64bits. Fondé sur les DES, sa clé a une taille variable, comprise entre 40bits et 448bits. Cet algorithme rapide et fiable.

Twofish

De la même manière que Blowfish, Twofish est un algorithme de chiffrement par bloc de 129bits sur 16 rondes, avec une longueur de clé variable. Il est également a la fois fiable et rapide.

AES (Advanced Encryption Standard)

AES est la nouvelle référence de cryptage. Fondé sur l'algorithme, Rijndael, c'est un algorithme par bloc de longueur variable extrêmement rapide. Actuellement utilisé par l'administration américaine en remplacement du DES et réputé pour sa fiabilité, AES a aussi été choisi comme nouvel algorithme de chiffrement pour la norme IEEE 802.11